IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL INC., a California corporation,	)	
Plaintiff,	)	
v.	)	Civ. No. 04-1199-SLR
INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, SYMANTEC CORPORATION, a Delaware corporation, and INTERNET SECURITY SYSTEMS, INC., a Delaware corporation,	)	
Defendants.	)	

Thomas Lee Halkowski, Timothy Devlin, Kyle Wagner Compton and John F. Horvath of Fish & Richardson, P.C., Wilmington, Delaware. Counsel for Plaintiff. Of Counsel: Katherine D. Prescott and Todd G. Miller of Fish & Richardson, P.C.

Richard L. Horwitz of Potter Anderson & Corroon, LLP, Wilmington, Delaware. Counsel for Internet Security Systems, Inc., a Georgia corporation. Of Counsel: Holmes J. Hawkins III and Natasha H. Moffitt of King & Spalding LLP, Atlanta, Georgia.

David Ellis Moore of Potter Anderson & Corroon, LLP, Wilmington, Delaware. Counsel for Internet Security Systems, Inc., a Delaware corporation. Of Counsel: Adam M. Conrad, Allison H. Altersohn, Charles A. Pannell, Latif Oduola-Owoo and Scott T. Weingaertner of King & Spalding, New York, New York.

Richard K. Herrmann and Mary Matterer of Morris James LLP, Wilmington, Delaware. Counsel for Symantec Corporation. Of Counsel: Goffrey M. Godfrey, Katie J.L. Scott, Paul S. Grewal, Renee Bubord Brown and Robert M. Galvin of Day, Casebeer Madrid & Batchelder LLP, Cupertino, California.

MEMORANDUM OPINION

Dated: August 21, 2008
Wilmington, Delaware

ROBINSON, District Judge

I. INTRODUCTION

Plaintiff SRI International, Inc. ("SRI") brought suit against defendants Symantec Corporation ("Symantec") and Internet Security Systems, Inc.[1] ("ISS") charging infringement of four patents: United States Patent Nos. 6,484,203 ("the '203 patent"), 6,708,212 ("the '212 patent"), 6,321,338 ("the '338 patent"), and 6,711,615 (the '615 patent"). Currently before the court is defendants' renewed motion for summary judgment that three of the four patents in suit are invalid pursuant to 35 U.S.C. § 102 and § 103.[2] (D.I. 297) The court's initial summary judgment determination was affirmed in part, and vacated and remanded-in-part, by the United States Court of Appeals for the Federal Circuit. (D.I. 491) The issues presently before the court were not reached previously and were renewed by defendants at the status conference held on April 29, 2008. (D.I. 504) For the following reasons, defendants' renewed motion for summary judgment of invalidity (D.I. 297) is denied.

II. BACKGROUND

The patents in suit relate to the monitoring and surveillance of computer networks for intrusion detection. In particular, the patents in suit teach a computer-automated method of hierarchical event monitoring and analysis within an enterprise network that allows for real-time detection of intruders. Upon detecting any suspicious activity, the network monitors generate reports of such activity. The claims of the '203

---

[1]There are two defendants sharing the name "Internet Security Systems, Inc.," one a Delaware corporation and one a Georgia corporation. For purposes of this opinion, they shall collectively be referred to as "ISS".

[2]The Federal Circuit affirmed the court's determination that the '212 patent is invalid as anticipated. (D.I. 491)

and '615 patents focus on methods and systems for deploying a hierarchy of network monitors that can generate and receive reports of suspicious network activity. To detect attacks which do not possess deterministic signatures or to detect previously unknown (new) attacks, the patents in suit disclose the use of statistical detection methods on network data. The claims of the '338 patent are directed to a particular statistical algorithm for detecting suspicious network activity.

Mr. Porras and Peter G. Neumann, on behalf of plaintiff, published a conceptual overview of the EMERALD system[3] in December 1996. (D.I. 301, ex. JJ) In October 1997, the authors published a more thorough account of the EMERALD system in *Emerald 1997*. (Id., ex. E) *Emerald 1997* was before the patent examiner during prosecution of the '338 patent, from whose application the remaining patents in suit were derived, and is listed as a reference on the face of the '615 patent. (Id., exs. A, B, & D) Within the text of *Emerald 1997* are twenty-four citations to outside references. (Id. at 365) Two of those references included the *Intrusive Activity 1991* reference.[4] (D.I. 301, ex. G) Mr. Porras is a named inventor on each of the patents in suit. (Id., exs. A-D)

III. STANDARD OF REVIEW

A court shall grant summary judgment only if "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any,

---

[3]The acronym "EMERALD" stands for Event Monitoring Enabling Responses to Anomalous Live Disturbances. (D.I. 507, ex. E)

[4]A publication entitled "A Method to Detect Intrusive Activity in a Networked Environment" ("*Intrusive Activity 1991*").

show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). The moving party bears the burden of proving that no genuine issue of material fact exists. See Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 586 n.10 (1986). "Facts that could alter the outcome are 'material,' and disputes are 'genuine' if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct." Horowitz v. Fed. Kemper Life Assurance Co., 57 F.3d 300, 302 n.1 (3d Cir. 1995) (internal citations omitted). If the moving party has demonstrated an absence of material fact, the nonmoving party then "must come forward with 'specific facts showing that there is a genuine issue for trial.'" Matsushita, 475 U.S. at 587 (quoting Fed. R. Civ. P. 56(e)). The court will "view the underlying facts and all reasonable inferences therefrom in the light most favorable to the party opposing the motion." Pa. Coal Ass'n v. Babbitt, 63 F.3d 231, 236 (3d Cir. 1995). The mere existence of some evidence in support of the nonmoving party, however, will not be sufficient for denial of a motion for summary judgment; there must be enough evidence to enable a jury reasonably to find for the nonmoving party on that issue. See Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 249 (1986). If the nonmoving party fails to make a sufficient showing on an essential element of its case with respect to which it has the burden of proof, the moving party is entitled to judgment as a matter of law. See Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986).

IV. DISCUSSION

A. Anticipation

A patent is anticipated under 35 U.S.C. § 102 if a single prior art reference explicitly discloses each and every limitation of the claimed invention. See SmithKline Beecham Corp. v. Apotex Corp., 403 F.3d 1331, 1343 (Fed. Cir. 2005). The prior art reference must be a printed publication, published more than one year prior to the date of the patent application in the United States. See Helifix Ltd. v. Blok-Lok, Ltd., 208 F.3d 1339, 1346 (Fed. Cir. 2000). The Federal Circuit has stated that "[t]here must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." Scripps Clinic & Research Found. v. Genentech, Inc., 927 F.2d 1565, 1576 (Fed. Cir. 1991). "In determining whether a patented invention is [explicitly] anticipated, the claims are read in the context of the patent specification in which they arise and in which the invention is described." Glaverbel Societe Anonyme v. Northlake Mktg. & Supply, Inc., 45 F.3d 1550, 1554 (Fed. Cir. 1995). The prosecution history and the prior art may be consulted "[i]f needed to impart clarity or avoid ambiguity" in ascertaining whether the invention is novel or was previously known in the art. Id. (internal citations omitted).

A prior art reference also may anticipate without explicitly disclosing a feature of the claimed invention if that missing characteristic is inherently present in the single anticipating reference. See Continental Can Co. USA v. Monsanto Co., 948 F.2d 1264, 1268 (Fed. Cir. 1991). The Federal Circuit has explained that an inherent limitation is one that is necessarily present and not one that may be established by probabilities or possibilities. See id. at 1268-69. That is, "'[t]he mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" Id. at 1269 (citations omitted). The Federal Circuit also has explained that "inherency operates to anticipate

entire inventions as well as single limitations within an invention." Schering Corp. v. Geneva Pharms. Inc., 339 F.3d 1373, 1380 (Fed. Cir. 2003). Recognition of the inherent limitation by a person of ordinary skill in the art before the critical date is not required to establish inherent anticipation. See id. at 1377.

An anticipation inquiry involves two steps. First, the court must construe the claims of the patent in suit as a matter of law. See Key Pharm. v. Hercon Labs. Corp., 161 F.3d 709, 714 (Fed. Cir. 1998). Second, the finder of fact must compare the construed claims against the prior art. See id. A finding of anticipation invalidates the patent. See Applied Med. Resources Corp. v. U.S. Surgical Corp., 147 F.3d 1374, 1378 (Fed. Cir. 1998). Issued patents are presumed valid, and the "underlying determination of invalidity . . . must be predicated on facts established by clear and convincing evidence." Rockwell Int'l Corp. v. United States, 147 F.3d 1358, 1362 (Fed. Cir. 1998) (citations omitted).

Defendants argue in their renewed motion for summary judgment that the so-called *JiNao Report* anticipates independent claims 1 and 24 of the '338 patent.[5] The

---

[5]Claim 1 discloses the following:

> 1. A method of network surveillance, comprising:
> receiving network packets handled by a network entity;
> building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the at least one measure monitoring data transfers, errors, or network connections;
> comparing at least one long-term and at least one short-term statistical profile; and
> determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

JiNao Report issued in April 1997 as part of a collaborative project[6] "aim[ed] at designing and developing a software system for protecting against intruders from breaking into network routers, switches, and network management channels." (D.I. 507, ex. F at 1) Although the stated goal of the project was to protect network infrastructure, the scope of the project was limited to "the development of local detection capabilities;" "detection conditions" were "confined to those that manifest on a local scale, specifically, those than can be observed somehow by neighboring entities."[7] (Id. at 12-13) To this end, the *JiNao* intrusion detection system intercepts and redirects "the target protocol information flow" to various modules for performance of both "statistical- and protocol-based intrusion checks." "Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be

---

Claim 24 discloses the following:

> 24. A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to:
>
> receive network packets handled by a network entity;
> build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets, the measure monitoring data transfers, errors, or network connections;
> compare at least one short-term and at least one long-term statistical profile; and
> determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

[6]The sponsors of the project were MCNC and North Carolina State University. (D.I. 507, ex. F)

[7]The court notes in this regard that defendants did not renew their motion for summary judgment on anticipation by the *JiNao Report* as to the asserted hierarchical claims of the '203 and '615 patents.

triggered." (Id. at 5) With respect to the "components of the statistical approach,"

> [a]spects of subject behavior are represented as measures (e.g., packet ...). For each measure, we will construct a probability distribution of short-term and long-term behaviors. For example, for the packet types received, the long-term probability distribution would consist of the historical probabilities with which different types of packets have been received, and the short-term probability distribution would consist of the recent probabilities with which different types packets have been received. In this case, the categories to which probabilities are attached are the names of packet types, which are learned by the system as they are received. We would classif[y] the Ji-Nao measures into two groups: activity intensity and audit record distribution measures. These two types of measures serve different dimensional purposes. The activity intensity measures determine whether the volume of general activity in the recent past . . . is normal. These measures can detect bursts of activity or prolonged activity that is abnormal, primarily based on the volume of audit data generated. The audit record distribution measure determines whether, for recently observed activity (say, the last few hundred audit records received), the types of actions being generated across neighbors are normal. For example, we might find that the last 200 routing packets received contained 120 of Hello packets, 15 of Database Description packets, 10 of Link State Request packets, 35 of Link State Update packets, and 20 of Acknowledgment packets. These data are compared to a profile of previous activity . . . to determine whether or not the distribution of activity types generated in the recent past (i.e., the last few hundred audit records) is unusual.

(Id. at 19)

The above paragraph illustrates the factual issue at bar. Although plaintiff concedes that the *JiNao Report* applied statistical methods and generated long-term and short-term statistical profiles, plaintiff argues that the data that formed the basis of these profiles was audit data, to be distinguished from "at least one measure of the network packets." (D.I. 507, ex. 1 at 25) The *JiNao Report* unquestionably refers both

to receipt of different "packet types"[8] and analysis of audit data/audit records.[9] (D.I. 507, ex. F at 19-20) Based on the record, it is unclear to the court[10] whether the *JiNao* intrusion detection system in fact builds its statistical profiles from at least one measure of network packets received, given that the scope of the *JiNao* project was limited to "the development of local detection capabilities." (D.I. 507, ex. F at 13) Because the scale of the *JiNao Report* arguably was different than that of the '338 patent, the court declines to find through a motion practice that the functions of the two systems (and semantics used to describe those functions) are exactly the same.

B. Obviousness

"A patent may not be obtained . . . if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art." 35 U.S.C. § 103(a). Obviousness is a question of law, which depends on several underlying factual inquiries.

> Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background the obviousness or nonobviousness of the subject matter is

---

[8]Recall that the court construed the term "packet" to mean "[a] group of data bytes which represents a specific information unit with a known beginning and end." (D.I. 468 at 2)

[9]The inventors of the '338 patent have described the prior art as focusing on "session activity within host boundaries," with "the primary input to intrusion-detection tools" being "audit data" "produced by mechanisms that tend to be locally administered within a single host or domain." (D.I. 407, ex. C at 2)

[10]In other words, defendants have failed to establish, by clear and convincing evidence, anticipation.

> determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented.

KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1734 (2007) (quoting Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966)). "Because patents are presumed to be valid, see 35 U.S.C. § 282, an alleged infringer seeking to invalidate a patent on obviousness grounds must establish its obviousness by facts supported by clear and convincing evidence." Kao Corp. v. Unilever U.S., Inc., 441 F.3d 963, 968 (Fed. Cir. 2006) (citation omitted).

"[A] patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." KSR, 127 S. Ct. at 1741. Likewise, a defendant asserting obviousness in view of a combination of references has the burden to show, by clear and convincing evidence, that a person of ordinary skill in the relevant field had a reason to combine the elements in the manner claimed. Id. at 1741-42. The Supreme Court has emphasized the need for courts to value "common sense" over "rigid preventative rules" in determining whether a motivation to combine existed. Id. at 1742-43. "[A]ny need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." Id. at 1742.

In addition to showing that a person of ordinary skill in the art would have had reason to attempt to make the composition or device, or carry out the claimed process, defendant must also demonstrate by clear and convincing evidence that "such a person would have had a reasonable expectation of success in doing so." PharmaStem

Therapeutics, Inc. v. ViaCell, Inc., 491 F.3d 1342, 1360 (Fed. Cir. 2007).

Defendants argue in their renewed motion for summary judgment that *Emerald 1997* in combination with an internally cited reference to *Intrusive Activity 1991* renders obvious the asserted claims of the '203 and '615 patents.[11] (D.I. 299 at 22) The

---

[11]Claim 1 of the '203 patent provides:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
> deploying a plurality of network monitors in the enterprise network;
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from the following categories: **{network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}**;
> generating, by the monitors, reports of said suspicious activity; and
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

(D.I. 508, ex. D) (emphasis added)

Claim 1 of the '615 patent discloses the following:

> 1. A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
> deploying a plurality of network monitors in the enterprise network;
> detecting, by the network monitors, suspicious network activity based on analysis of network traffic data selected from one or more of the following categories: **{network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgments, and network packets indicative of well-known network-service protocols}**;
> generating, by the monitors, reports of said suspicious activity; and
> automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

(Id.) (emphasis added)

limitation at issue is that of particular categories of network traffic. According to defendants, it would have been obvious in light of the express teaching in *Emerald 1997* to analyze those network traffic categories based upon the citation to *Intrusive Activity 1991*. (D.I. 299 at 23) The court, therefore, must determine whether: (1) *Intrusive Activity 1991* disclosed one of the claimed categories of network traffic data; and (2) there was a reason to combine *Emerald 1997* with *Intrusive Activity 1991*.

With respect to *Intrusive Activity 1991*, the following are disclosed: (1) intrusion detection systems "examine available sources of information;" (2) the main source of information for most intrusion detection systems is the audit trail generated by the operating system; (3) observation of network packets, however, can also be used as a basis to detect intrusive activity through a system description language ("SDL"); (4) the SDL provides a structure that allows for the generalization of basic objects to detect complex objects and assigns meaning to those objects to determine whether intrusive activity is present; (5) basic objects, "similar to terminal symbols in traditional programming languages," are packets;[12] (6) complex objects are composed of basic objects and/or other complex objects and can include a "stream" of packets; (7) a "stream" is a complex object type which defines a process and includes the "number of packets exchanged" between two processes; (8) "[o]nce the structural grammar, attributes, and attribute functions have been defined, a second set of functions, called behavior-detection functions, must be defined for each object in the structural grammar," allowing for a determination regarding whether the object is associated with

[12]"Basic objects for other systems may be an audit record from an operating system." (D.I. 508, ex. D (*Intrusive Activity 1991* at 367))

intrusive activity. (D.I. 508, ex. D) (*Intrusive Activity 1991* at 363-69)

Defendants argue that *Intrusive Activity 1991* specifically disclosed analysis of the claimed network traffic data category "network packet data volume." (D.I. 500 at 2 n.3) Defendants, however, provide no expert testimony in support of this assertion, relying solely on the text.[13] Plaintiff argues that this text concerns the syntax for creating a descriptive language that provided the general framework for the Network Security Monitor ("NSM") and, in this regard, proffers Dr. George Kesidis' testimony.[14] (See D.I. 507, ex. J at ¶ 40) More specifically, plaintiff asserts that the "cited language says literally nothing about using packet data volume to detect suspicious activity."[15] (D.I. 502 at 2) Based on the above, it is unclear to the court whether the discussion of "network packet data volume" contained in *Intrusive Activity 1991* sufficiently discloses to one having ordinary skill in the art that this parameter could be used to detect

---

[13]The discussion of the alleged "network packet data volume" occurs in a section describing the "SDL" and not in the later section, which discusses the second set of functions called "behavior-detection functions." (See D.I. 508, ex. D (*Intrusive Activity 1991* at 368-69))

[14]Wherein he states: "[N]ot only does the combination [of *Emerald 1997*, *Intrusive Activity 1991* and *NIDES 1994*,] not disclose every limitation, but also one of ordinary skill in the art would not have been motivated to combine these disparate references." Although arguably conclusory, Dr. Kesidis does refer the reader to his prior discussion of the NSM system as disclosed in *Intrusive Activity 1991* and *Emerald 1997*, which is consistent with plaintiff's argument that the NSM approach teaches away from the claimed inventions. (See D.I. 507, ex. J at ¶ 40; D.I. 507, ex. J at ¶¶ 22-44, 53-60)

[15]This argument is not contained in plaintiff's original summary judgment brief. (See D.I. 507, ex. 1 at 12-14) Although the court cautioned against new arguments at the status conference, this assertion is an extension of plaintiff's overall argument that a NSM, which describes monitoring local area networks, is fundamentally different from enterprise networks, the subject of the patents in suit. (See D.I. 507, ex. 1 at 13; D.I. 502 at 2)

suspicious network activity such that the limitation at issue is rendered obvious.

Defendants' argument that *Intrusive Activity 1991* discloses network connection "requests" and "denials" also does not persuade the court that summary judgment is warranted. Relying on the text of *Intrusive Activity 1991*, which states that "network connections are created and destroyed continuously," defendants simply assert that "[o]ne of ordinary skill would have understood this disclosure of analyzing the creation and destruction of network connections to disclose monitoring network connection requests and network connection denials." (D.I. 508, ex. B at 31-32) As with the alleged disclosure of "network packet data volume," the court is not comfortable with granting summary judgment where the meaning of the text to a person having ordinary skill in the art is unclear.[16] In other words, a genuine issue of material fact exists regarding what a person having ordinary skill in the art would interpret the disclosure in *Intrusive Activity 1991* to convey.

V. CONCLUSION

For the reasons stated, defendants' renewed motion for summary judgment (D.I. 297) is denied. An appropriate order shall issue.

[16]Having determined that summary judgment is inappropriate, the court will not address the parties' arguments with respect to the motivation to combine element.